AIR WAR COLLEGE

AIR UNIVERSITY

CYBER SITUATIONAL AWARENESS

FOR

JOINT FORCE COMMANDERS

by

Kevin M. Payne, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 February 2012

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Kevin M. Payne is a U.S. Air Force Cyber Officer assigned to the Air War College, Air University, Maxwell AFB, AL. Lt Col Payne is a graduate of Ohio University with a Bachelor of Science degree in Electrical Engineering and entered the Air Force in 1991 through the Reserve Officer Training Corps. He also has a Master's Degree in Management from Central Michigan University in 1999. His experience includes Airborne Warning and Control System (AWACS) computer operations, War Planner for the 9th Air Force Central Command Headquarters, Communications Squadron Commander at Ramstein Air Base, Germany and Squadron Commander at the Joint Communications Support Element. Lt Col Payne has also served as the Chief, Network Operations for the Joint Staff at the Pentagon.

Abstract

The United States Military's joint warfighting concepts for the operational and tactical levels must be closely examined to ensure forces can create a shared information environment within the cyber domain that is effective enough to support joint military operations in a timely manner. The central thesis being addressed is that military commanders need a common framework for cyber situation awareness in order to aid the force with building a robust information sharing environment. Two key cyber mission areas–Cyber Support and Cyber Engagement–along with their associated cyber functional capabilities are described with the purpose of emphasizing their importance to conducting joint operations. This research explores the essential role that operational command centers have in creating an effective information environment. Also, a mental model for cyber situation awareness is provided based on four primary information sources: (1) Cyber Support, (2) Cyber Engagement, (3) Joint Force Leadership, (4) Cyber Commons. Using analysis from the model, three primary challenges are also discussed along with proposed solutions.

Introduction

Military commanders rely on situational awareness (SA) to understand the operational environment, synchronize actions, combat adversaries and make decisions on projecting military power. Although the four physical domains–land, sea, air, and space–are relatively mature with regard to joint military operations, the new cyber domain creates a significant challenge with combatting ever-increasing threats. In response, the United States (US) Military launched initiatives to improve its cyber capabilities through organizational, procedural and technological changes. Strategic-level changes, such as establishing US Cyber Command (USCYBERCOM) and its associated service-level components were an essential first step to producing greater cyber capabilities. However, joint warfighting concepts for the operational and tactical levels of combat must be closely examined to ensure forces can create a shared information environment within the cyber domain that is effective enough to support specific joint military operations in a timely manner.

The central thesis being addressed is that military commanders need a common framework for cyber SA in order to aid the force with building a robust information sharing environment. Included in this research is background on SA followed by a description of the Joint Force Commander's (JFC) information environment and their importance to military operations. Next, two key cyber mission areas, *Cyber Support* and *Cyber Engagement*, along with their associated cyber functional capabilities are described regarding their importance to joint operations. A mental model for cyber SA is presented which is based on four primary information sources: (1) Cyber Support, (2) Cyber Engagement, (3) Joint Force Leadership, and (4) Cyber Commons. Finally, using analysis from the model, three primary challenges are discussed with proposed recommendations.

Background

Situational Awareness is about knowing what is going on around you and, ideally, being able to anticipate what will happen. Dr. Mica Endlsey's research on SA provides a common definition which is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[1] According to her model, SA has three levels: (1) Perception, (2) Comprehension, and (3) Projection. Through our senses, a person gathers data and information in order to perceive a particular situation. By mentally processing the perceived information, one can comprehend the situation at a particular level of understanding. With additional cognition focused on thinking ahead in time, individuals can make forecasts of future events that may occur. The model characterizes a larger process of repeatedly sensing the environment, assessing the situation and deciding on future actions in order to ultimately achieve the desired objective. Endsley's SA model is a useful tool for researchers and also has similarities with Colonel Boyd's OODA Loop.

Commonly used within the US Military community, the OODA Loop is a theoretical model based on situational awareness and decision-making. Conceptualized by the US Air Force pilot and combat veteran Col John Boyd, the mental model's four primary steps–Observe, Orient, Decide, and Act–are repeated in a continuous loop.[2] A core principle is that through mental swiftness and ingenuity, warfighters must out think their adversary and outmaneuver them in ways that will disrupt their adversary's OODA Loop decision cycle.[3] The first two OODA Loop steps—Observe and Orient—are vital for producing SA information, which can, in turn, enable effective decision-making during step three. A warfighter with higher levels of SA compared to an equally matched adversary can create a military advantage. However, warfighters operate in a challenging environment in which there are many obstacles to maintaining effective SA.

Three common obstacles to maintaining effective SA are complex situations, limitations in cognitive capacity and poor information sharing. Complex situations, such as coordinated night operations in hostile environments require highly trained and experienced military personnel in order to adequately comprehend the circumstances.[4] Limitations in memory capacity and multi-tasking abilities create barriers where essential information will not be perceived and processed fast enough to deal with a rapidly changing environment.[5] Poor information sharing results in a team member not receiving essential information which reduces the degree of shared SA and overall team effectiveness.[6] These obstacles and others contribute to create the *Fog of War* which is a concept popularized by writings from the 19th Century military strategist Carl von Clausewitz. He described a mental fog caused by the uncertainty of data, contradictory information and peculiarities of the mind.[7] Although commanders know information can be unreliable, building an effective information environment can help to reduce the fog of war.

Cyber Information Environment

For Joint Force Commanders, the information and operational environments are highly interdependent. Military commanders rely on the information environment to help them understand the *operational environment* which is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.[8] The *information environment* is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information (which includes the information itself).[9] The information environment resides between the physical and cognitive environments and enables individuals the ability to perceive the world around them.[10] Cyberspace is part of the information environment, which has had a significant influence in increasing the amount of data and information available for people and organizations.

Cyber SA relies on information from multiple sources. Four primary information source groups are shown in figure 1 which includes the following: (1) Joint Force Leadership, (2) Cyber Support, (3) Cyber Engagement, and (4) Cyber Commons. These four groups feed into the shared information environment and their specific interactions will be discussed in the following sections.

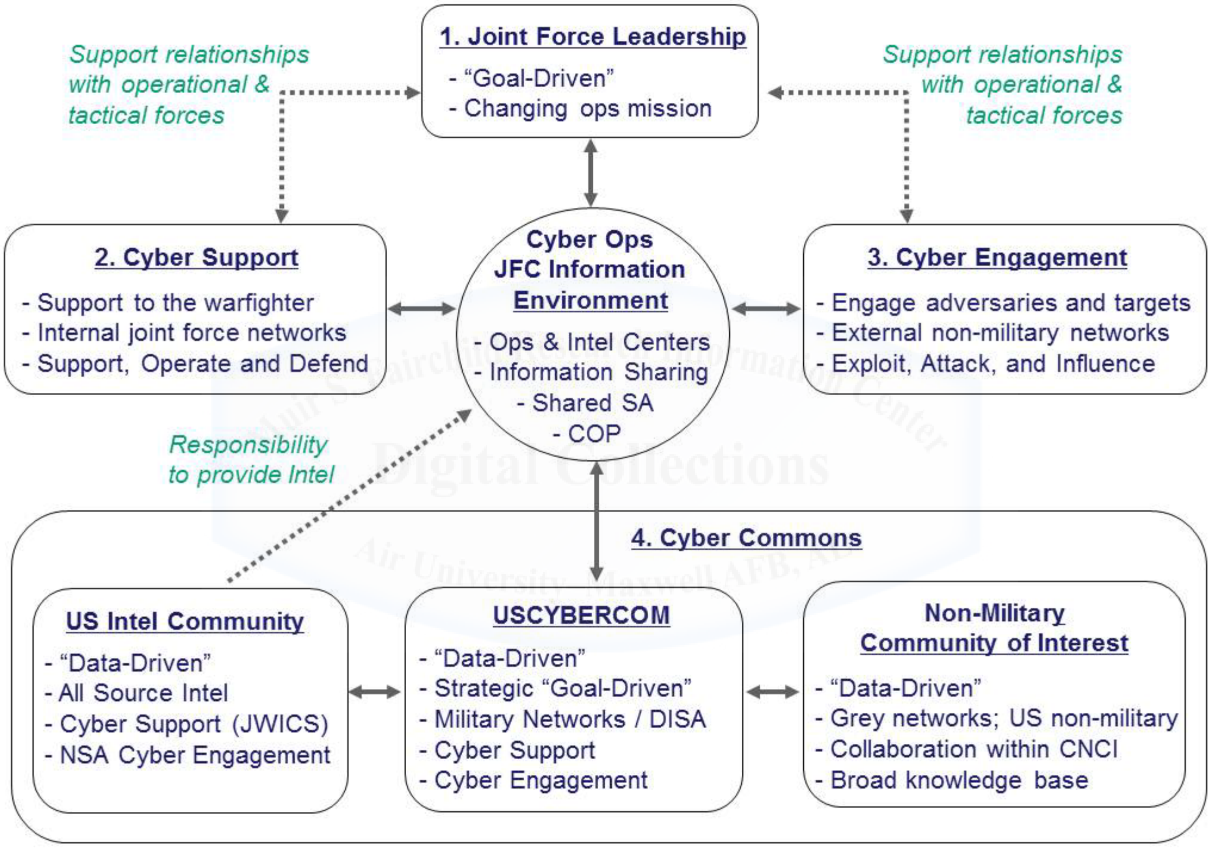
1. Joint Force Leadership
- "Goal-Driven"
- Changing ops mission
Support relationships with operational & tactical forces
Support relationships with operational & tactical forces
2. Cyber Support
- Support to the warfighter
- Internal joint force networks
- Support, Operate and Defend
Cyber Ops JFC Information Environment
- Ops & Intel Centers
- Information Sharing
- Shared SA
- COP
3. Cyber Engagement
- Engage adversaries and targets
- External non-military networks
- Exploit, Attack, and Influence
Responsibility to provide Intel
4. Cyber Commons
US Intel Community
- "Data-Driven"
- All Source Intel
- Cyber Support (JWICS)
- NSA Cyber Engagement
USCYBERCOM
- "Data-Driven"
- Strategic "Goal-Driven"
- Military Networks / DISA
- Cyber Support
- Cyber Engagement
Non-Military Community of Interest
- "Data-Driven"
- Grey networks; US non-military
- Collaboration within CNCI
- Broad knowledge base

Figure 1. Joint Force Cyber SA Information Sources

Staff personnel and command centers consolidate information from multiple sources. By serving as a continuously operating information hub, command centers maintain SA of the operational environment and provide capabilities for command and control (C2). Depending on the mission, commanders may have a single command center or multiple centers within their headquarters. For example, J2, J3 and J6 staff directorates will each manage their respective intelligence center, operations center, and network operations center. Utilizing multiple centers benefits each staff directorate with maintaining their own tailored systems and processes. However, multiple centers with different focus areas often leads to information being stored in different locations resulting in a fractured information environment and limited SA.

Compartmentalizing information hinders the ability to see parallel operations that are simultaneously occurring. In order to gain full SA, JFCs need to receive information that is fused together from the common cyber functions (see figure 2). Especially with regard to USCYBERCOM and its service components, there is an effort between Cyber and Intel organizations to better fuse information between functional operations.[11] Even through the cyber information environment appears simple, the four source categories do not necessarily integrate easily into a cohesive picture. Common issues that exist are compartmentalization between offices, security classification differences, and resistance to information sharing.

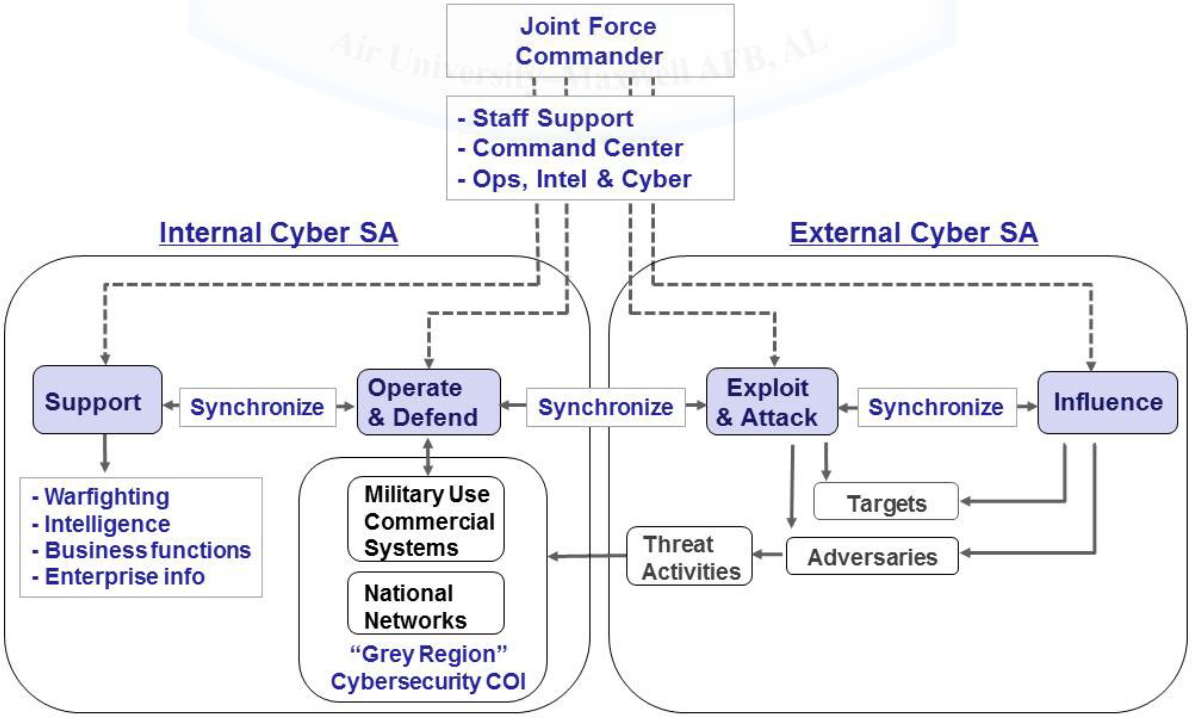

Figure 2. Cyber SA Information Sources

Internal and External Cyber Regions

Commanders rely on cyberspace for two primary requirements which are: (1) enable effective operational capabilities and decision-making, and (2) engaging actors in the operational environment in order to achieve mission objectives. These two requirements reflect the two mission area concepts of Cyber Support and Cyber Engagement. Taking the concept further, Cyber Support functions focus on the joint force's internally managed networks, whereas Cyber Engagement functions focus on the adversary's networks which are external to the joint force. The information in Table 1 details differences between the Cyber Support and Cyber Engagement mission areas.

Table 1. Internal and External Joint Cyber Mission Areas and Functions

Cyber Mission Area	*Cyber Function*	*Description*
Cyber Support (Internal)	Support	Service Support. Includes actions taken to service requirements for personnel, weapon systems and organizations to ensure optimum performance, network connectivity, and access to dedicated, tactical or enterprise-level cyber capabilities.
	Operate	Operate & Maintain (O&M). Includes actions taken to ensure networks are reliable, responsive and can quickly recover if subject to an unauthorized outage.
	Defend	Computer Network Defense (CND). Includes actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity.[12]
Cyber Engagement (External)	Exploit	Computer Network Exploitation (CNE). Intelligence collection, processing and assessments conducted through the use of computer networks are done to gather data from target or adversary networked systems.[13]
	Attack	Computer Network Attack (CNA). Use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks.[14]
	Influence	Engage key audiences to create, strengthen or preserve conditions favorable to meeting US Government interests, policies and objectives.[15]

In order to gain sufficient SA in the joint force's operational environment, the primary cyber activities must be combined. Military commanders need to combine the information from Cyber Support functions (i.e. internal network-focused) and Cyber Engagement functions (i.e. external network-focused). The cyber mission areas and functions described in this research are a composite of terminology used in various doctrinal sources. At the present time, the Joint Staff is reviewing at least 16 different doctrine documents in order to better articulate cyberspace operations which is projected to be in a new document designated as Joint Publication 3-12, *Cyberspace Operations*.[16] Although terms will be revised based on new doctrinal guidance, the broad concepts used in this study are still useful in characterizing the activities within the cyber operations environment. Cyber Support is the mission area that JFCs rely on most since it is essential to sustaining forces in the field.

Cyber Support – Internal Cyber Region

For many years, the predominant requirement for military communicators was to support warfighters' requirements, operate military communications systems and defend the systems from attack in order to enable effective joint operations. The US Army describes tactical communications as part of Combat Service Support.[17] Whereas, the US Air Force uses the concept Agile Combat Support. Although described differently through the lens of service-specific terminology, military communicators are essential to providing Cyber Support to the warfighter. The Joint Communications Support Element (JCSE) is a Cyber Support unit with the unique mission of providing direct support to Regional Combatant Commands (COCOM), Joint Task Forces (JTF), Special Operations Command, and other agencies.[18]

JCSE effectively delivered Cyber Support capabilities for the US Southern Command (USSOUTHCOM) during Operation UNIFIED RESPONSE. On 12 January 2010, Haiti suffered a catastrophic earthquake and the US military responded quickly in providing humanitarian assistance. As the supported regional COCOM, USSOUTHCOM oversaw the effort and established JTF Haiti to manage the on-site operations. JCSE communicators deployed to Haiti and ensured that the JTF headquarters element had the essential communications and C2 capabilities needed for their command center. Prior to their troops deploying to Haiti, JCSE communicators, in coordination with USSOUTHCOM/J6, immediately began building a virtual Joint Network Operations Control Center (JNCC) with a dedicated website, network monitoring displays and operational planning information.[19] In addition, JCSE utilized its JNCC responsibilities to have deploying units share their network status information to create a common operational picture (COP) of the tactical network. JCSE's support during UNIFIED RESPONSE emphasize how Cyber Support is essential to providing cyber SA of internal military networks and serves as the glue for holding joint operations together. In contrast to internal networks, the emergence of USCYBERCOM demonstrates the need for greater SA of external networks.

Cyber Engagement – External Cyber Region

The second mission area for joint cyber operations is Cyber Engagement which includes activities in cyberspace directed at adversaries and operational targets. In military terms, *Engagement* is a tactical conflict, usually between opposing lower echelon maneuver forces.[20] By projecting military power through various kinetic and non-kinetic means, forces engage adversaries and targets to achieve mission objectives. Non-kinetic engagements, such as Information Operations (IO), provide the US Military with the ability to influence actors in the operational environment without using direct military action. As an essential capability, IO relies on computer network operations to shape the information environment through exploit, attack and influence functional capabilities. Cyber Engagement activities are focused on networks outside of the US Military's own infrastructure and directed towards systems utilized by adversaries and potential targets. As cyberspace becomes more prevalent around the globe and adversaries continue to exploit its vulnerabilities, the US Military will increasingly rely on Cyber Engagement to deter adversaries and achieve operational objectives.

The US Department of Defense's (DoD) establishment of USCYBERCOM and its integration with the Intelligence Community (IC) shows the US Military's resolve in utilizing Cyber Engagement as a essential element to warfare. On 21 May 2010, the USCYBERCOM reached initial operational capability and officially took the lead for the DoD's cyber operations. The command is charged with centralizing cyberspace operations, strengthening DoD cyberspace capabilities, and integrating and bolstering DoD's cyber expertise.[21] USCYBERCOM's commander is also in charge of the National Security Agency (NSA), which enables better integration of Title 10 cyber activities through the military services with America's Title 50 electronic intelligence gathering capabilities. The command is making substantial investments in building Cyber Engagement capabilities, such as the new USCYBERCOM Joint Operations Center (JOC). The JOC is part of an overarching $3 billion site expansion in conjunction with NSA at Fort Meade, Maryland.[22] USCYBERCOM's new cyber capabilities and initiatives to improve operational synergy will significantly enhance America's ability to project military power through cyberspace. As the US Military's lead cyber organization, the command serves as the prime integrator for Cyber Support and Cyber Engagement functional capabilities.

Joint Force Commanders will increasingly rely on Cyber Support and Cyber Engagement as key lines of operation in order to improve warfighting effectiveness. Through methods such as horizontal fusion, information from disparate sources can be integrated to create a broader view of cyber activities occurring in parallel from across the cyber domain. By slicing information horizontally from the six common cyber functions–support, operate, defend, exploit, attack, and influence–cyber and intelligence support forces can generate a comprehensive view of the cyber operations in progress. Combining information horizontally from across internal and external cyber regions is essential to providing cyber SA, and the next section addresses the vertical synergy needed between top-level goals and bottom-level data.

Top-Level Goals and Bottom-Level Data

Situational Awareness requires a combination of top-down and bottom-up assessments for maintaining an eye on changing leadership goals and events in the operational environment. Top-level goals and bottom-level data are important factors that shape the information environment. Military forces must stay alert to identify changes in goals and data that will result in changes in the operational environment. Top-down (goal-driven) information processing enables a person to focus their attention on the primary objective which helps in establishing more detailed priorities and compare information relevant to mission accomplishment.[23] In contrast, bottom-up (data-driven) processing is able to catch someone's attention while not specifically looking for the information.[24] Data-driven information is import for identifying changes in the environment that were not expected. Alternating between top-down (goal-driven) and bottom-up (data-driven) scanning is vital for maintaining SA.

Joint Force Leadership – Top-Level Goals

Military commanders have the essential responsibility to provide the primary goals, objectives and operational approach to accomplish the overall mission requirements. In order to handle the span of control over distributed forces and build a comprehensive operational picture, commanders require a significant amount of information from situation reports. They also need to assess the perceived situation, make decisions and issue orders which must be distributed in a timely manner. Without commanders providing clear goals for mission accomplishment, their people will have limited ability to prioritize tasks, organize information and focus attention on how best to achieve the desired objectives.

Military commanders, like Gen Omar Bradley, relied heavily on their staff personnel, command post (CP), and communications system in order to maintain an effective information environment. During World War II, General Bradley was the12th Army Group field commander when the German Ardennes Offensive began. His CP and staff were located in Luxembourg when the Germans broke through Allied lines.[25] Concerned about General Bradley's position being overrun and losing essential communications equipment, General Eisenhower recommended that he relocate to Verdun, France. Bradley decided to stay while a parallel communications system was established in Verdun as a contingency. General Omar Bradley emphasized the importance communications in his book *A Soldier's Story*:

> With division, corps and Army staffs schooled in the same language, practices and techniques, we could resort to sketchy oral orders… Those orders ... were transmitted easily over the most valued accessory of all — the elaborate telephone system we carried with us into the field. From my desk in Luxembourg I was never more than 30 seconds by phone from any of the Armies. If necessary, I could have called every division on the line. Signal Corps officers like to remind us that "although Congress can make a general, it takes communications to make him a commander." The maxim was never more brilliantly evidenced than in this battle for the Ardennes.[26]

From General Bradley's experiences in the Battle of the Bulge, there are at least two notable observations. First, commanders along with their staff and command center are an essential part of the information environment. As a headquarters element, they need the best information possible in order to adequately perceive the situation, out thinking their adversary and create a superior strategy. Second, the CP was useless without a reliable communications system to enable information gathering and issue orders back out to the units. Despite being taken by surprise with a substantial force, the Allies were agile enough in their decision-making OODA Loop to effectively use their maneuver forces in pushing back the German offensive. This historic event highlights the need for an agile information environment that can quickly adapt to a rapidly changing operational environment. Furthermore, this requirement continues to be a vital necessity through all generations of military professionals.

Military commanders still rely on their staff and command center for maintaining an effective information environment. Advancements in communications technologies have increased the ability for conducting network-centric operations in which forces can self-synchronize. However, the operational environment has also grown significantly more complex in which the commander’s guidance is often necessary for determining the desired operational approach. In contrast to top-level goals which help focus attention towards specific objectives, forces must process bottom-level data for understanding the evolving operational environment.

Cyber Commons – Bottom-Level Data

The internet provides a substantial amount of information which can be used to a military’s advantage, but it can also cause many distractions. Much like finding a needle in a haystack, cyber operators can be overwhelmed with scanning data and conducting forensics in order to identify malicious activity. The US DoD has more than 15 thousand networks that consist of 7 million devices and 20 thousand commercial circuits.[27] In addition, unauthorized users probe the DoD's networks about 250 thousand times an hour.[28] Data-driven processing is used to identify events that should raise alarms, threat warnings and generate indicators which increase awareness of critical changes in the operational environment. Much like a house alarm to signal a burglary, some common monitoring devices for cyberspace include tracking system outages, computer viruses, and network intrusions. Another useful device that is designed to aggregate data from the environment is a COP.

Military forces utilize the COP as a tool to process large amounts of data in order to create a visual representation of the operational environment. On 3 June 2010, USCYBERCOM's first commander Gen Keith Alexander, stated that "We must first understand our networks and build an effective cyber situational awareness in real time through a common, sharable operating picture."[29] The COP is a single display of relevant information shared by more than one command to achieve SA.[30] Although a single display is certainly preferred, the many disjointed US military and coalition networks require numerous tools used by highly trained experts. Currently, operational forces can only build a COP to see only a small fraction of the total cyber domain. In addition, military Cyber and Intel organizations do not operate in a virtual environment that can be easily labeled in black and white (i.e. military and non-military systems). In-between internal military networks and external non-military networks is the grey region.

Military commanders face challenges with the grey region where US forces are not permitted to monitor for SA. The grey region described in this research paper includes American owned networks, or other cyber regions, where the US military is legally restricted from gathering information. America's Intelligence Community is not permitted to conduct intelligence gathering on private citizens which limits the US Military's Cyber Engagement capabilities for defending against attacks emanating from within the US. Since adversaries can use US networks to mask the true origin of an attack, this region of cyberspace can be a blind spot for military cyber operations.

The US Government established the Comprehensive National Cybersecurity Initiative (CNCI) as a complimentary solution to the problem in which organizations with different authorities in cyberspace are able to share information. The CNCI requires dedicated cyber operations centers to establish information exchange and collaborate to enhance cyber SA.[31] Also, the CNCI provides the DoD with additional resources of information in order to identify and combat cyber threats. Conversely, the DoD is utilizing its defensive capabilities the ability to assist in determining the state of US networks and systems. The fourth cyber information source group is called the *Cyber Commons* because it is a resource shared among a large collection of organizations. The collective information environment shared between various military and non-military organizations provide a community of interest (COI) that is dedicated to ensuring the right for common use within cyberspace. USCYBERCOM serves as the DoD's lead in supporting the JFC's access and reliance to the cyber commons.

Recommendations

As the US Military works to incorporate the cyber domain into its warfighting environment, it faces some unique challenges with improving the manner in which it manages its operational information. The first challenge is establishing a framework for joint operations that will enable the military services to have greater unity of effort in regard to Cyber Support and Cyber Engagement. The second challenge is for the military services to have a set of common functional capabilities necessary for joint cyber operations that reinforces interoperability and establish baseline performance standards. The third challenge is ensuring military operations centers are able to fuse the necessary information to create a COP that can enrich the quality of real-time information processing. The following three challenges are discussed with proposed recommendations.

Formalize a framework for joint cyber operations

Establishing a joint cyber SA framework can serve to create a common mindset for cyber operations and enhance partnerships across all levels of command. Joint doctrinal changes currently in progress will help to improve operational synergy, but that alone is insufficient. Joint doctrine will not address fundamental issues with building partnerships. For example, America's Intelligence Community not only implemented organizational changes after 9/11, but it also promoted a change in mindset. In 2008, the IC adopted a new information sharing model encouraging replacement of the *Need to Know* approach to one centered on a *Responsibility to Provide*.[32] The recommended change in attitude was an effort to reverse the practice of restricting intelligence information, and instead push information out to where it was needed in support of mission requirements.

Similarly, organizations in the cyber community rely on partnerships to be effective, but they often restrict outside access. For example, cyber units routinely deny requests for external access into their networks or provide bandwidth for other organizations unless specifically directed by a higher authority. The tradeoffs between requirements for a robust joint force network and those of its service components are regularly at odds with each other. Although cyber units must responsibly manage risk, they cannot engage in too much risk avoidance which can impact the joint force's ability to share information. As part of a new framework, cyber units need a mindset where Cyber Support and Cyber Engagement go beyond immediate organizational needs. The joint community would benefit by also insisting on greater expectations for sharing network access in order to improve areas such as consolidating network monitoring. In addition to improved interoperability, the issue of security classification limits information sharing.

The mission areas of Cyber Support and Cyber Engagement are mutually supporting and together provide a cohesive picture of the cyber operational environment. However, organizations conducting Cyber Engagement activities tend to operate at a higher security classification level than those performing Cyber Support. Different security levels are necessary, but too much over-classification can create unnecessary gaps in knowledge and blind spots that diminish the force's collective SA. As addressed previously, the information sharing between internal military networks and external non-military networks is vital to the overall information environment. In addition to internal and external synergy for improving cyber SA, joint force headquarters need to assess their approach to handling goals (top-down) and data (bottom-up).

Reinforce using the six common cyber functions for joint operations

Building the cyber SA framework based on the six common joint cyber functions described in this research would provide a core set of common functional capabilities in support of joint operations. The US military services maintain considerably different training certifications, network architectures and performance standards for network operations. If the six functions—support, operate, defend, exploit, attack, and influence—were reinforced within service capabilities, the joint community could more easily develop a functional model for executing joint military operations in cyberspace. Ensuring military services can support the core functions will encourage more interoperability through mutually-shared processes and capabilities.

Although the US military services maintain capabilities tailored to suit their specific mission responsibilities, the common cyber functions provide a foundation for cyber operations in support of joint military operations. For example, US Air Force combat communicators are organized, trained and equipped to provide expeditionary Cyber Support as well as maintaining air traffic control (ATC) systems for expeditionary sites. While ATC is an important capability for airfield operations, it is not directly related to cyber operations. The different mission areas emphasize how the various cyber forces should present their capabilities in comparison to Cyber Support and Cyber Engagement frameworks. The capability comparisons can determine how well particular cyber organizations can fit within a structured joint cyber operations architecture.

In addition, horizontally slicing of information from across the six parallel functional areas can provide a broader view of the cyber operational environment for joint force leadership. Dispersed joint forces working independent of each other usually have little incentive to provide a broad brush view of their cyber operations. With an effective strategy to provide SA information based on the six primary cyber functions, a JFC should have greater understanding of the environment. The disjointed nature in which cyber operations can be parsed out creates problems in building an effective information environment. So, establishing common standards for reporting on the primary functions will improve assimilating status information from multiple forced dispersed across a region.

Posture Operations, Intelligence and Command Centers for cyber war

The US Military may not know exactly when a major cyber attack will occur, but it should be postured to adequately respond to one. Just as General Bradley's staff quickly reacted during the Battle of the Bulge, today's command elements require the same agility for ensuring the information environment keeps pace with a highly dynamic operational environment. In cyber warfare, capable adversaries can simultaneously execute numerous attacks crippling major portions of America's military, government, commercial and infrastructure systems. Since massing forces is not required and vulnerabilities can be secretly exploited over time, enemy combatants would likely have the element of surprise. During crisis events and when engages in combat operations, command centers serve as the vital location for managing information.

Operations, Intelligence and Command Centers serve as a critical hub in building the information environment to assist commanders with understanding the operational environment and communicating directives once decisions are made. However, the complexity of coordinating between the large array of functional centers (i.e. Cyber, Operations, and Intelligence, etc.) that exist across the US Military's strategic, operational and tactical levels of command can contribute to considerable confusion. Therefore, the information environment should reside in networks where it is easily shared among multiple operations and intelligence centers. Command centers should organize information around goals and effectively transmit the goals to the supporting forces in a manner that enables unity of effort. If possible, cyber forces should provide information that is already processed instead of merely forwarding raw data so that teams can more quickly gain comprehension (Level 2 SA) of the situation. In addition, cyber forces should avoid sending large amounts of data that will only hinder progress and reduce the command center's OODA Loop.

The Joint Force Command and the USCYBERCOM Commander are the two primary sources of top-level goals for conducting joint cyber operations. The JFC provides goals from an operational-level perspective, whereas USCYBERCOM provides goals from a strategic level. It is important for the JFC and USCYBERCOM to have synergy with establishing goals for Cyber and Intel forces in order to ensure that activities do not diverge result in operational disconnects. Also, a JFC expecting to focus solely on the physical domains and leave the cyber domain to USCYBERCOM is a mistake in taking for accountability for the operational environment. JFCs must also take into account that regarding cyber operations, USCYBERCOM is the supported command and it has the lead for determining the operational approach unless changed by a higher authority.

Conclusion

If a military force is effectively managing its information, its leadership will be able to maintain higher levels of perception and comprehension that will result in a greater understanding of their operational environment. The ability for the information environment to effectively provide shared situational awareness depends on how a Joint Force Commanders is able to bring together cyber operational forces, command centers and information systems. Through formalizing operations around the Cyber Engagement and Cyber Support mission areas along with their associated cyber functions, a Joint Force Commander will be able to more effectively integrate capabilities, respond to changing conditions and maintain situational awareness of the cyber domain.

Bibliography

Alexander, Keith. CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of the U.S. CYBERCOM, Washington, D.C. Center for Strategic International Studies (CSIS), 3 June 2010.

Arquilla, John, "The New Rules of War", *Foreign Policy*, March/April 2010.

Bousqet, Antoine. *The Scientific Way of Warfare*. New York, NY: Columbia University Press, 2009.

Bradley, Omar N., General. *A Soldier's Life*. New York: Henry Holt & Co., 2002.

Endsley, Mica R, Bolte, Betty, and Jones, Debra G. *Designing for Situation Awareness*. Boca Raton, FL: Taylor & Francis Group, 2003.

Clausewitz, Carl von. *On War*, Project Gutenberg. 25 February 2006 (resourced at http://www.gutenberg.org/files/1946/1946-h/1946-h.htm#2HCH0006 on 1 February 2012).

Gladwell, Malcolm. *Blink, the Power of Thinking Without Thinking*. New York, NY: Bay Back Books, 2005.

Information Sharing Strategy, Washington D.C.: United States Intelligence Community, 2008.

Joint Communications Support Element (JCSE). JCSE Home Website. (resourced at http://www.jcse.mil/live09/index_n.htm on 15 January 2012).

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 October 2011).

Joint Publication 3-13, *Information Operations*, 13 February 2006).

Joint Staff Program Directive (PD) for Joint Publication 3-12, Cyberspace Operations. 13 October 2011 (resourced at http://www.dtic.mil/doctrine/new_pubs/jointpub.htm on 20 October 2011).

Hickey, Andrew R. “Gen Alexander at RSA: Cyber Security a ‘Team Sport’ ”. CRN Magazine. February 17, 2011. http://www.crn.com/news/security/229218902/gen-alexander-at-rsa-cyber-security-a-team-sport.htm.

Larsen, et al. *Understanding Commanders’ Information Needs for Influence Operations*. Santa Monica, CA: RAND Corporation, 2009

Osinga, Frans P.B. *Science, Strategy and War, the Strategic Theory of John Boyd*. Abingdon, Oxon: Routledge, 2007

Public Intelligence Website. “NSA $3.2 Billion “Site M” Expansion Planning Documents Reveal Cyberwar Command Center”. 14 June 2011 (resourced at http://publicintelligence.net/nsa-site-m-cybercom/ on 1 February 2012)

Jajodia, Sushil, Peng Liu, Vipin Swarup, Cliff Wang. *Cyber Situational Awareness, Issues and Research*. Heidelburg, London: Springer, 2010

United States Strategic Command. “US Cyber Command Fact Sheet”, 23 June 2009 (resourced at http://www.stratcom.mil/factsheets/Cyber_Command/ on 1 February 2012).

White House, Comprehensive-National-Cybersecurity-Initiative, (resourced at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative on 15 November 2011)

Notes

[1] Endsley, *Designing for SA*, 13

[2] Osinga, *Science, Strategy and War, the Strategic Theory of John Boyd*, 229-233

[3] Ibid., 230

[4] Endsley, *Designing for SA*, 39

[5] Ibid., 36

[6] Ibid., 197

[7] Clausewitz, *On War*, 2006, Chapter II Section 24

[8] Joint Publication 1-02, *Department of Defense Dictionary*, 246

[9] Ibid., 160

[10] Joint Publication 3-13, *Information Operations*, I-2

[11] Gen Keith Alexander, Briefing Center for Strategic International Studies, 3 June 2010

[12] Ibid., 65

[13] Ibid., 65

[14] Ibid., 67

[15] Larsen, *Understanding Commanders' Information Needs for Influence Operations*, xiv - xx

[16] Joint Staff Program Directive for Joint Publication 3-12, 13 October 2011

[17] Joint Publication 1-02, *Department of Defense Dictionary*, 57

[18] JCSE Home Website, http://www.jcse.mil/live09/index_n.htm, 15 January 2012

[19] First-hand account from the author while assigned to JCSE

[20] Joint Publication 1-02, *Department of Defense Dictionary*, page 114

[21] US Cyber Command Fact Sheet, http://www.stratcom.mil/factsheets/Cyber_Command/

[22] Public Intelligence Website, http://publicintelligence.net/nsa-site-m-cybercom/ , 14 June 2003

[23] Endsley, *Designing for SA*, 25

[24] Ibid.

[25] Bradley, *A Soldier's Life*, 466

[26] Ibid., 473

[27] Gen Keith Alexander, Briefing Center for Strategic International Studies, 3 June 2010

[28] Ibid.

[29] Ibid.

[30] Joint Publication 1-02, *Department of Defense Dictionary*, page 48

[31] White House National Security Council, www.whitehouse.gov, 15 Nov 2011

[32] US Intelligence Community, *2008 Information Sharing Strategy*, 9